

AFFIDAVIT

I, Patrick Hanna, being duly sworn, depose and state as follows:

Introduction

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and currently assigned to the Burlington Resident Agency in Vermont. I have been an FBI Special Agent for 19 years. My duties as an FBI Special Agent include investigating violations of Title 18 of the United States Code as they pertain to corporate fraud, complex financial crimes, embezzlement, public corruption, money laundering and related white-collar crimes, as well as violent crimes and criminal enterprises. I have participated in investigations of criminal violations of various federal laws. I have executed search and arrest warrants, interviewed and interrogated subjects, witnesses, and victims, and conducted surveillance. In the course of these investigations, I have gained an understanding of current technology, to include computers and online accounts, cellular telephones and associated records and data, and have conducted analyses of the data related to such accounts and devices, for the purpose of solving and proving crimes.

2. I make this affidavit in support of an application for a search warrant authorizing the examination of an electronic device – a white Samsung Galaxy Note 3, currently in the custody of the Vermont State Police in Waterbury, Vermont, further described in Attachment A (Subject Device) – and the extraction of electronically stored information described in Attachment B.

3. As discussed below, there is probable cause to believe that Jerry Banks was involved in the kidnapping and murder of Gregory Davis, whose deceased body was discovered on January 7, 2018. There is probable cause to believe that Davis' kidnapping and murder involved the following federal crimes: kidnapping, in violation of 18 U.S.C. § 1201, murder to obstruct justice, in violation of 18 U.S.C. § 1512(a)(1); and murder for hire, in violation of 18 U.S.C. § 1958. There is probable cause to believe that device described in Attachment A contains evidence of those crimes.

4. This case is being investigated by the FBI and the Vermont State Police (VSP). Since this affidavit is being submitted for the limited purpose of establishing probable cause to search data already in law enforcement's custody, I have not included details of every aspect of the investigation. Except as otherwise noted, the information contained in this Affidavit is based upon my personal knowledge and observations, my training and experience, conversations with other law enforcement officers and witnesses, and my review of documents and records.

Probable Cause

5. On March 30, 2022, I obtained a Criminal Complaint from this Court charging Jerry Banks with the kidnapping of Gregory Davis in violation of 18 U.S.C. § 1201(a)(1).

6. On April 6, 2022, I applied for and obtained a search warrant for the premises of 1179 Pfothenhauer Road, Fort Garland, Colorado (hereafter "Residence Warrant"), a property owned by Jerry Banks. The affidavit in support of that search warrant was based in large part on

my complaint affidavit. A copy of my affidavit submitted in support of the Residence Warrant is attached as Exhibit 1 and is incorporated here.

7. As set forth in more detail in Exhibit 1, there is probable cause to believe that prior to his murder, Davis was the victim of a financial fraud scheme involving Serhat Gumrukcu and his brother, Murat Gumrukcu. This financial fraud scheme involved investments in an oil trading company, and agreements between Murat Gumrukcu's entity Laurant Trading, LLC; Gregory Davis' entity Mode Commodities, LLC; and Gregory Gac's entity Quadrant Financial Group, LLC (functioning as an "escrow agent" for the parties).

8. As set forth in Exhibits 1, there is probable cause to believe that Jerry Banks murdered Davis, and that he was hired to do so on behalf of a third party. As set forth in Exhibit 1, the only known link between Banks and the Gumrukcus is through Aron Ethridge and Berk Eratay.

9. On April 6, 2022, Jerry Banks was arrested in Yellowstone National Park. On April 7, 2022, FBI agents executed the Residence Warrant at Banks' property in Colorado. During the search, in the trailer-type residence, agents located 9mm ammunition; a hand-held radio; two firearm magazines; a green law-enforcement style duty belt; and a Seagate Expansion Desktop Drive. In a storage shed, agents recovered a short-barrel AR-15 with no serial numbers or manufacturer labels; an AR-15 "upper" (no lower receiver) with a scope; handcuffs; a pepper blaster; and a FedEx envelope containing purchase paperwork and registration for a Ford Explorer from Highline Automotive. In a maroon Chevy Blazer located on the property, agents recovered a vehicle spotlight, which was disassembled into two pieces.

10. On April 7, 2022, I interviewed Aron Ethridge near his home in Henderson, Nevada. During this initial interview, Ethridge denied all knowledge of a murder-for-hire scheme involving Banks. On the morning of April 9, 2022, I received a call from Ethridge, who agreed to meet again later that day. At this second meeting, Ethridge admitted he had lied during the first meeting, and then confirmed the murder-for-hire scheme involving Banks and Eratay. A third meeting with Ethridge was held on April 10, 2022, during which Ethridge admitted he had omitted some of his knowledge of the plan to abduct Davis during his interview on April 9. The following is a summary of the information that Ethridge provided to law enforcement during the April 9 and April 10 interviews, with corrections as provided by Ethridge on April 10:

- a. Ethridge and Eratay used to be neighbors in Henderson, Nevada, and became friends during that period.
- b. Eratay approached Ethridge over a year before the murder of Davis, asking if Ethridge could arrange a murder. Ethridge eventually agreed to assist Eratay.
- c. Ethridge approached Banks, asking Banks to assist with the murder.

d. Ethridge received over \$110,000 in cash from Eratay as payment for the murder. A portion of this cash was paid to Banks.

e. The initial plan had been for Banks to “snipe” Davis, but after Banks made a reconnaissance trip to Vermont, Banks advised the plan would have to be revised and requested additional payment due to the increased difficulty of the job.

f. Ethridge knew that Banks would impersonate a law enforcement officer and abduct Davis from his residence prior to murdering him.

g. Ethridge and Banks communicated via an encrypted application called “Threema.” Ethridge also communicated with Eratay on the “Threema” application.

h. On at least one occasion, Banks used a physical data card to pass along a digital image of Davis that Banks had taken during a trip to Vermont. Ethridge provided this data card to Eratay.

i. On January 7, 2022, while Banks was traveling back from Vermont, Banks called Ethridge and advised him the job was done. Ethridge then called Eratay to relay the message.

j. Ethridge had met Serhat Gumrucku on multiple occasions prior to the murder of Davis. Ethridge believed that, based on these meetings and statements made by Eratay, Serhat was the man who wanted Davis killed. Eratay told Ethridge that Serhat had a problem with Davis and asked Ethridge to help them get rid of the problem. However, Serhat and Ethridge never directly communicated about the abduction and murder. All communications went through Eratay, who Ethridge knew to work for Serhat.

k. After the murder of Davis, Eratay provided Ethridge with an additional payment in the form of Bitcoin.

11. On June 29, 2022, I spoke with Jami Machovec, who lived with Banks at the Fort Garland residence from mid-2016 to March 2017 and again from April 2018 to mid-2018. Machovec provided information to me about Banks’s role in the murder after receiving an agreement that her statements would not be used against her. Prior to this agreement, she had minimized her knowledge about and assistance with the murder plot. In summary, Banks admitted to Machovec that he had been hired to murder Davis, that he had taken a trip to Vermont to surveil Davis, and that he took a video of Davis while on this reconnaissance trip. Machovec reported that Banks showed her the video on his computer while visiting her in Dexter, Missouri, and that Banks asked her to assist him in the kidnapping of Banks by posing as Banks’s law enforcement partner when Davis was “arrested.” Machovec said that the video appeared to have been filmed through some sort of scope. Machovec agreed to accept delivery in Dexter of several items Banks planned to use in the murder. Machovec told me that when she left

Colorado in mid-2018, she took cellphones from the residence she lived in with Banks. One of those devices was a Samsung Galaxy Note 3. She told me that she did not use this phone. She thought it was one of Banks's phones. Machovec agreed to turn the Samsung Galaxy Note 3 over to law enforcement.

12. In July 2022, Machovec provided the Samsung Galaxy Note 3 to a law enforcement office in the area where she lived. That officer sent this device, the Subject Device, to Todd Baxter of the Vermont State Police, which has the phone in custody in Vermont.

13. As noted in Exhibits 1, I have reviewed records relating to Banks's Amazon purchases in 2017. Those records show that on October 15, 2017, Banks purchased a scope with a smart phone attachment that allowed a user to take smartphone pictures or videos on a smartphone trained through the scope.

14. I have reviewed information obtained from a search warrant of Google account banksavs@gmail.com, Banks's account. Google was recording location data for an unidentified device from at least January 2017 to September 8, 2017. The last Google location data point for that unidentified device is a WIFI router at or near the Costilla County Sheriff's Office in San Luis, CO, on September 8, 2017, at 06:51:23 UTC, which converts to 11:51 PM MDT on September 7, 2017. As described in Exhibit 1, Jerry Banks was employed by the Costilla County Sheriff's department at that time. The Google email data shows that the user made a new sign in for the Google account on September 8, 2017 at 11:13 AM GMT, which converts to 5:13 AM MDT on September 8, 2017, for a Samsung Galaxy Note 3. A representative of the Costilla County Sheriff's Office has told law enforcement that Banks worked the "graveyard" shift as a jail guard.

15. During the course of investigation, I have reviewed Verizon phone records for the 661 Phone, described in Exhibit 1. The phone records show that the Subject Device provided to law enforcement by Machovec has the same IMEI number as the 661 Phone used by Banks in 2017, including while Banks travelled to Vermont in November 2017. The Verizon records show that this phone was used in connection with the Verizon All Valley Solar account beginning in December 2014. Machovec confirmed to me that Banks worked for All Valley Solar in December 2014. I believe that Banks continued to use the Subject Device even when he was not working for All Valley Solar, that he possessed and used this phone during the time the murder scheme was being planned and executed, and that it contains evidence as described in Attachment B.

Electronic Storage and Forensic Analysis

16. Based upon my training and experience, and my discussions with other law enforcement officials, I know the following:

a. Users of digital devices increasingly choose to store items in digital form (e.g. pictures or documents) because digital data takes up less physical space, and can be easily

organized and searched. Users also choose to store data in their digital devices because it is more convenient for them to access data in devices they own, rather than to later spend time searching for it. Keeping things in digital form can be safer because data can be easily copied and stored off site as a failsafe.

b. Users also increasingly store things in digital form because storage continues to become less expensive. Today, one terabyte (TB) hard drives are not uncommon in computers. As a rule of thumb, users with one gigabyte of storage space can store the equivalent of 500,000 double spaced pages of text. Thus, each computer can easily contain the equivalent of 500 million pages, that, if printed, would fill six 35' x 35' x 10' rooms. Similarly, a one TB drive could contain 900 full run movies, or 900,000 songs, or four million images. With digital devices, users can store data for years at little cost to no cost.

c. Storing data in digital form and not deleting it mirrors users' online habits where users have, for many years, been encouraged to never delete their emails. For example, since June 2007, Google, Inc. has promoted free, increasingly larger storage "so you should never have to delete mail." *See* Bill Kee, *Welcome to Official Gmail Blog*, <https://gmail.googleblog.com/2007/06/welcome-to-official-gmail-blog.html> (July 3, 2007); *see also* Rob Siembroski, *More Gmail Storage Coming For All*, <https://gmail.googleblog.com/2007/10/more-gmail-storage-coming-for-all.html> (Oct. 12, 2007) (promoting its "Infinity+1" plan to constantly give subscribers more storage).

d. Digital devices can also store data automatically, without a user's input. For example, network logs may track an employee's actions for company auditing purposes or email headers may automatically list the servers which transmitted the email. Similarly, a web browser (i.e. an application such as Internet Explorer used to access web pages) can track a user's history of websites visited so users can more easily re-access those sites. Browsers also temporarily cache files from recently accessed web pages to improve the user's experience by reducing that page's loading time. These examples illustrate how the interaction between software and operating systems often results in data being stored without a user's knowledge. Even if a sophisticated user understands this automatic storage of data, attempts at deleting this data often fail because the data may be automatically stored multiple times and in different locations. Thus, digital evidence may exist despite attempts at deleting it.

e. Digital data is practically resilient to deletion. First, as noted, data is often automatically stored multiple times in multiple locations, where even sophisticated users may not be able to locate. Second, digital data can be recovered years after it has been saved, or viewed even after such data has been deleted. For example, when a user deletes a file on a computer, the file is sent to the recycle bin, where it can still be retrieved. Even if the file is deleted from the recycle bin, the data does not actually disappear; rather it remains in "free space" or "slack space" (i.e. in unused space) until it is overwritten by new data. Third, an operating system may also keep deleted data in a "recovery" or "swap file." Fourth, files from websites are automatically retained in a temporary cache which is only overwritten as they are

replaced with more recently viewed web pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer use habits.

17. Based on my training, my experience, and information provided to me by those involved in the forensic examination of digital devices including cell phones, I know that completely segregating information before an examiner has started reviewing digital evidence is inconsistent with the evidence assessment process. This is true for the following reasons:

a. This application seeks permission to locate and seize not only data that might serve as direct evidence of the Subject Offenses, but also for evidence that establishes how digital devices were used, the purpose of their use, and who used them. Additionally, this application seeks information about the possible location of other evidence.

b. This application seeks permission to search and seize evidence, fruits, or instrumentalities found in the device described in Attachment A. Some of these items may be files and other data that is generated by a user (e.g. documents, pictures, and videos). Alternatively, other items may be device generated data that becomes meaningful only upon forensic analysis. For example, as noted, a hard drive may contain records of how a computer was used, the purposes for which it was used, and who has used these records. These items are the subject of this warrant.

c. For instance, based upon my training, my experience, and information provided by others involved in the forensic examination of digital devices, I know the following: First, as noted, data that is not currently associated with any file can provide evidence of a file that once existed, but which has since been deleted or altered. This can include a deleted portion of a file (e.g. a paragraph deleted from a document). Second, applications such as web browsers, email, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Third, operating systems can record information, such as the attachment of peripherals (e.g. USB flash drives), and the times the device was in use. Similarly, file systems record the dates files were created and the sequence in which they were created. Any of this information may be evidence of a crime, or indicate the existence and location of evidence in other locations on the digital device.

d. In determining how a digital device has been used, the purpose for which it was used, and who has used it, it is sometimes necessary to establish that a particular thing is not present. For example, in cases where more than one person has used a digital device, agents can infer that a defendant must have been the person who used that device to commit a crime by eliminating the possibility that other people used that device during that time. Because file systems often list the dates and times those files were created, this information can help exclude the possibility that other people were using that digital device. As another example, by reviewing a computer's Index.dat files (a system file that keeps track of activity conducted in Internet Explorer), a forensic examiner can determine whether a user accessed other information

close in time to the file creation dates, times, and sequences so as to establish user identity and exclude others as having used that computer during times related to the criminal activity. Demonstrating the significance of the absence of certain data on a digital device may require analysis of the digital device as a whole.

e. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a user or excluding a user. All of these types of evidence may indicate ownership, knowledge, and intent.

f. This type of evidence is not “data” that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

18. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

19. Based on my training, my experience, and information given to me by others involved in the forensic examination of digital devices, I know that searching for this kind of evidence involves technical, complex, and dynamic processes, which may require expertise, specialized equipment and a knowledge of how digital devices are often used to commit the Subject Offenses.

20. There is probable cause to believe that things that were once stored on the Subject Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files

downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

21. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

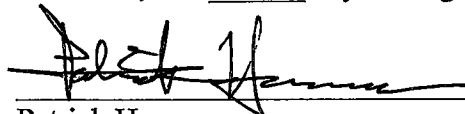
e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. The Subject Device has been stored in such a manner that the data on it likely remains in the same condition as when law enforcement first seized it.

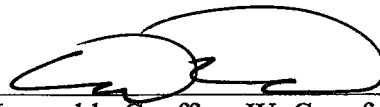
23. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41. The proposed search warrant would authorize the government to conduct a forensic examination of the Subject Device. Because the government already has custody of the Subject Device, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Dated at Burlington, in the District of Vermont, this 5th day of August 2022.


Patrick Hanna
Special Agent - FBI

Sworn to and subscribed before me this 5 day of August 2022.


Honorable Geoffrey W. Crawford
United States District Judge